

# Cloud Computing

**Kartikey Pokhriyal**

B. Tech Student

Department of Computer Science

Maharaja Agrasen College, University of Delhi

*Abstract*— Cloud computing today is known to be the game changing technology in the IT industry. With the ever increasing data and hardware required to manage it, cloud is a boon to all. It allows resource sharing that includes software, platform and infrastructure by means of virtualization. Virtualization is the core technology behind cloud resource sharing. This environment strives to be dynamic, reliable, and customizable with a guaranteed quality of service. Cloud vendors like Amazon, Microsoft Azure, IBM provide a variety of services. Elastic computing cloud and S3 (Simple Storage Service) are services provided by amazon. This paper basically is an understanding of cloud is and its working, along with Cloud Views which is a technology being worked upon. Also security of cloud which is the major concern of the present hour is also discussed.

**Key words:** Cloud Computing, CloudViews, IP spoofing

## I. INTRODUCTION

Cloud computing are on demand services, you pay for what you use. It's a broad and deep platform that helps to store large chunks of data, building application and providing virtualised machines.

You can store data and applications on remote servers and access them via internet rather than saving or installing them on your personal or office computer.

### A. Types of Services

Pay for what you use! Yes this is how convenient cloud is. But what all services it provides is something which would be explained next.

#### 1) SaaS (Software as a Service)

Applications, or the so called apps we are familiar with, cloud provides with apps for different needs of customers. Most applications can be run from the web browser itself one doesn't take the load of installing it. Mailing services are a familiar and widely used example-Gmail provides you with mailing services, also you can edit or create documents, spread sheets, presentations using Google play services without really installing Microsoft office.

#### 2) PaaS (Platform as a Service)

It provides you with a framework to build your applications. You get an Operating system, programming language execution environment, databases, web servers etc. for you work. Generally used to test, develop and deploy your application which otherwise is very tedious. For example: Windows azure, Google app engine etc.

#### 3) IaaS (Infrastructure as a Service)

It provides you with computing infrastructure like virtual machines, firewalls, virtual local area network etc. Instead of having to purchase hardware users can purchase IaaS based on consumption, similar to electricity bill. Example: Amazon Web Services, Windows Azure etc.

### B. Working

We know what cloud is and what services it can provide, but how does the entire system of cloud computing works? Basically there is a front end and a back end, the former is from where we access the cloud or the client's machine and the latter is what is called our cloud. Front end consists of basic software on the client's machine needed to access the data or applications, stored and provided by the cloud. While on the back end is a cluster of servers, data storage system, computers that create the cloud of cloud computing system. A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called middleware.

Initially client sends service requests, after the request is received the system management finds the correct resources and then finally the request of client's services are sent back.

### C. Types of Clouds

Now there are some ways in which you can categorize cloud and they are public, private and hybrid. Different customers have varied needs and hence exist such types-

#### 1) Public Cloud

The services are provided over the internet in public cloud by different cloud providers like amazon. They show great level of efficiency in shared resource. These services can be accessed and used by common masses. It is an obvious choice when-

- Your application is used by a large number of people like mailing services
- You need to test and develop your application code
- You're doing collaboration projects

### 2) Private clouds

A private cloud is one in which the services and infrastructure are maintained on a private network. These clouds offer the greatest level of security and control, but they require the company to still purchase and maintain all the software and infrastructure, which reduces the cost savings. It's an obvious choice when:

- Your business is your data and your applications. Therefore, control and security are paramount.
- Your business is part of an industry that must conform to strict security and data privacy issues.

### 3) Hybrid Clouds

A hybrid cloud includes a variety of public and private options with multiple providers. By spreading things out over a hybrid cloud, you keep each aspect at your business in the most efficient environment possible. The downside is that you have to keep track of multiple different security platforms and ensure that all aspects of your business can communicate with each other.

### D. CloudViews

With ever increasing number of web services managing databases through traditional means is cumbersome. We all use applications of varied kinds daily and most of them are under the same cloud. With CloudViews the objective is to collaborate with these services which would eliminate the problem of space and bandwidth. Obviously you won't collaborate a messaging app with a reading app i.e. collaboration would be done on the basis of common uses and that both would work together to synergize the effect. CloudViews is one kind of function public clouds must offer to facilitate web service development. How that can be done? This is what we discuss further.

- 1) Mashups are advancement in this field, which are nothing but collaboration of different web services making things easy for us.
- 2) Client-side Mashups: They are called so as the contents of the composing services are aggregated in client's browser. Example: Ola cabs app used these days displays the automobiles available at the moment around you.
- 3) Server-side Mashups: Mashups site aggregates information from other services and its own database and returns data to the client. Example: Facebook

### E. The Free and Fast Network

In traditional systems different web services have their own databases. Communication among these services are done over high-delay, low-bandwidth and expensive WAN's. With the advent of public clouds they can enjoy a fast and high-bandwidth inter web service network.

All the data for web services will be placed at the same location or the same cloud hence its fast and there won't be much delay. Amazon for example has S3 (Simple Storage Service) service in which the user can rent data and whosoever wishes to access the data has to pay a fee for it with the authentication query feature.

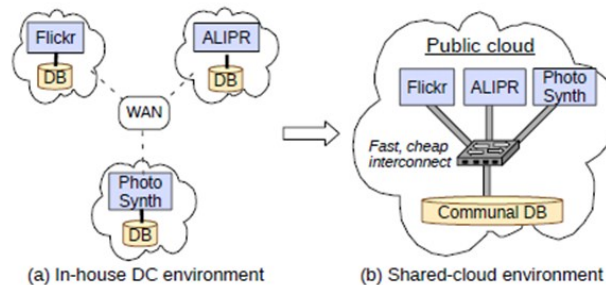


Fig. 1: The free and fast network

In figure 1 you can see Flickr (photo sharing service storing over 3 billion photos), ALIPR (automatic tagging of photos using image recognition), Photosynth (3D-scene re-composition from photos) services operating currently in their own databases. Mashing them up together in a public cloud as shown in fig. 3(b) because of the common use will be beneficial in terms of fast network and common storage. For example: Photosynth leverages Flickr to create 3D models from photos of tourist attractions. Similarly, Flickr could benefit from ALIPR, which could automatically add tags to its photos.

### F. The View Abstraction

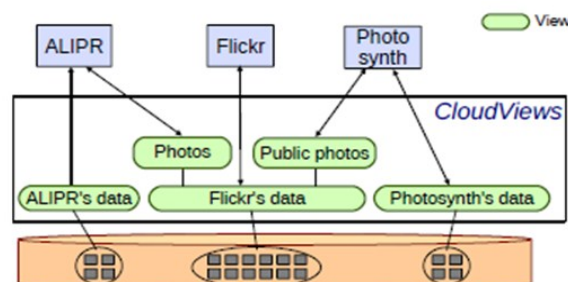


Fig. 2: Data sharing in CloudViews

Fig. 2: explains as to how the collaboration works. Every web service has its own view with its label that means no one else can access its data defined by that view except it itself. For example Flickr has its view by the name 'Flickr's data' which only it but no one else can access. So one might think if this is the case how do these services collaborate? It's like if some

web service wants to it can provide its view or a part of it to some other party. As we can see in fig. 4 Flickr provides photos as a view to ALIPR and not its personal database, ALIPR can use the view to tag those pictures. Similarly Photosynth has been provided the view public photos.

### G. Where Else Can This Be Implemented?

The example explained makes us ponder as to where else this technology or the idea can be used. One of the places is search engine!! Yes, why not? It's the most frequently visited place by everyone so why not have some upgrades in it. For instance Websites for varied services can provide their view to the search engine and every time websites update or upload some content the search would get the information about the same, thus aiding search engines to gather stuff.

Protection in case of cloud views would be done by self-certifying a view by cryptographic signature which would tell that the web-service has the full access to that particular view and no other party can tamper it unless it is certified for the view as well.

Although measure like self-certifying view will be taken but still it cannot be fully secure due to the reasons discussed further.

## II. CLOUD AND SECURITY

Security of cloud is one of the major concerns today, though cloud providers have come with solutions but still 100% safety can't be assured even today. Below are some threats to cloud today-

### A. Cloud Hijacking

In cloud hijacking the attacker takes full control of your account by breaking into it. Now he/she could use it for some bad purpose and can affect your data considerably.

To aid the above problem we can adopt the following tactic-

#### 1) Get Notified

The main threats to cloud environment are mainly data hijacking or loss of data. Company's records, some business transaction, or someone's personal data, nothing is entirely safe within the cloud custody. Data is an integral part and any tampering with it can cause havoc to the company. Threats like DOS (Denial of Service), IP spoofing, Cross-side VM attack are also dreaded by the cloud users.

So then? Can we breathe or rely with such attacks prevalent now and then, obviously NO! Well assessing the conditions one of the possible solution could be notifications. How? Well the main purpose would be to notify user whenever someone logs into his/her cloud account. Every party who has some or the other data residing in the cloud has to authenticate his/her identity before accessing it, but nothing stops a hacker to hack.

Elaborating further, if you're a cloud user and every time you log into to your account a notification would be sent to your cell phone on the registered cell phone no., one will have the complete details of the log(IP address, timings)with the notification. So you can just verify the notification every time 'you' log into your account. Simple? Well what if you receive your notification when you're attending a party? I think you got the indication and also that this remedy is basically to alert you, so if such condition arises an option to deny your log would be provided along with it which would lead into disabling your account for an hour or so. This way you can save your account at the very instant someone breaks into it.

The discussed measure was in context of an individual but what if it's a lot of employees? Well, in that case every time an employee logs in the boss will get a notification and the IP address would be of the network of their company, so the person would know that it's safe and allow the passage.

We have some other threats too which can cause a state of havoc-

### B. Man in the Middle Attack

This attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.

### C. IP Spoofing

Spoofing is the creation of TCP/IP packets using somebody else's IP address. Intruder gain unauthorized access to computer, whereby he sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

### D. Instance Isolation

As we know cloud providers can provide us with required no. of virtual machines, though the no. of instances or VM's at your device are isolated but if there is some VM with any malicious virus along with it, other VM's on the same machine can get affected. The so infected VM can even enter to your own system and extract your resources and tamper your privacy.

Cloud providers have come up with some measures to tackle these problems -

#### 1) SAML (Security Assertion Markup Language)

It is an XML based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. It verifies the user upon his/her entering into the system who provides the identity and is verified by the service provider.

#### 2) OpenID

In this the identity of the customer or the user of cloud can be verified by the provider or the provider can ask some third party to do so. In that case the cloud providers provide only the services but the authentication is done by some other party.

### III. CONCLUSION

Cloud Computing has brought a revolutionary change in the IT industry, with its pay for what you use policy it has become convenient and flexible to the users. Looking from a business perspective this can really aid start-ups who are not ready to invest money into hardware and software purchases. CloudViews as one of the future technologies discussed if implemented can lead to efficiency in terms of storage and speed. Different Web-services with common features can join hands to synergize a common goal over high-bandwidths. However flexible, convenient the cloud is but the security issues leaves it under scepticism. But from time to time cloud providers come up with remedies to fix things up. This technology has strengthened its roots in the IT industry and today almost everyone is moving towards clouds.

### REFERENCES

- [1] <https://en.wikipedia.org/wiki/OpenID>
- [2] [https://en.wikipedia.org/wiki/Security\\_Assertion\\_Markup\\_Language](https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language)
- [3] <http://www.business.com/cloud-computing/4-cloud-advancements-coming-in-2015/>
- [4] <https://www.computenext.com/blog/when-to-use-saas-paas-and-iaas/>
- [5] [https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CCIQFjABahUKEwjk5tOp-NDHAhXHSY4KHd\\_BDQw&url=https%3A%2F%2Fwww.usenix.org%2Fevent%2Fhotcloud09%2Ftech%2Ffull\\_papers%2Fgeambasu.pdf&ei=zwjVatDMceTuQTfg7dg&usg=AFQjCNE3rCVVs2zs0qmEFvu-EaJtrmZ80g](https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CCIQFjABahUKEwjk5tOp-NDHAhXHSY4KHd_BDQw&url=https%3A%2F%2Fwww.usenix.org%2Fevent%2Fhotcloud09%2Ftech%2Ffull_papers%2Fgeambasu.pdf&ei=zwjVatDMceTuQTfg7dg&usg=AFQjCNE3rCVVs2zs0qmEFvu-EaJtrmZ80g)